UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,360	09/28/2000	Thomas Guthrie Zimmerman	ARC9-2000-0091-US1	7556

7590 05/07/2004

Samuel A Kassatly
6819 Trinidad Drive
San Jose, CA 95120

EXAMINER	
HO, THOMAS M	
ART UNIT	PAPER NUMBER
2134	3

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/672,360	**Applicant(s)** ZIMMERMAN, THOMAS GUTHRIE	
	Examiner Thomas M Ho	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 September 2000_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-39_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-39_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. **Claims 1-39 are pending.**

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1-9, 19-31, 33-39 rejected under 35 U.S.C. 102(a) as being anticipated by De La Huerga, US patent 5,960,085.

In reference to claim 1.

De La Huerga discloses a tracking system for use with an identification medium to provide time-limit access to a resource, comprising:

- A transmitter module secured to the identification medium; (Column 9, lines 20-33)
- A receiver module in selective communication with the transmitter module; (Column 9, lines 34-49)
- The transmitter module including an encryptor and a time generator that generates a temporal sequence of values(TBn), wherein the encryptor encrypts the temporal

sequence of values (TBn) with a private key Kn which is unique to the identification medium to generate a code list composed of encrypted node elements (TBn) Kn, and wherein the transmitter module transmits one or more encrypted code elements (TBn)Kn to the receiver module; where the time generator generates the sequence of values as timestamps (Column 21, lines 45-50) & (Column 19, lines 17-33), and where the code list of encrypted elements is the list of the timestamps and other information on the smartcard used to form the audit trail (Column 19, lines 49-64), and where this information is encrypted on the with the private key (Column 16, lines 7-15)

- A server, connected to the receiver module, for storing the private key of the identification medium, and including an authenticator that authenticates one or more of the encrypted code elements of the code list, where the private keys may be stored on a separate security verification system or on computer terminal 60, itself. (Column 12, lines 33-39)

In reference to claim 2:

De La Huerga discloses the tracking system according to claim 1,

- for use with a plurality of identification media, each identification medium including a transmitter module (Column 9, lines 32-50), where the identification media has a transmitter module
- and a unique private key for transmitting at least one or more of the encrypted code elements(TBn)Kn to the receiver module for authentication. (Column 11, lines 10-15)

In reference to claim 3:

De La Huerga (Column 12, lines 33-39) discloses the tracking system according to claim 2, wherein the server stores private keys of the plurality of identification media, where the private keys may be stored on a separate security verification system or on computer terminal 60, itself.

In reference to claim 4:

De La Huerga (Column 11, lines 30-45) discloses the tracking system according to claim 3, wherein the receiver module provides unidirectional communication with at least one of the plurality of identification media, where the receiver component is designed to take part in the signal path with a transmitter. A communication path consisting of the a transmitter and receiver component is inherently unidirectional.

In reference to claim 5:

De La Huerga (Column 13, lines 19-35) discloses the tracking system according to claim 3, wherein upon authenticating the identification medium, the authenticator provides authentication information to an application for initiating the application.

In reference to claim 6:

De La Huerga (Column 11, lines 20-22) discloses the tracking system according to claim 3, wherein the private key is represented by a bit-string having a length of at least 48 bits, where the private key is at least 128 bits.

In reference to claim 7:

De La Huerga (Column 13, line 65 – Column 14, line 29) discloses the tracking system according to claim 5, wherein the transmitter module transmits the encrypted code elements at a predetermined transmission cycle, where the predetermined transmission cycle is the periodic polling with recommitment signals.

In reference to claim 8:

De La Huerga(Column 13, lines 37-50) discloses the tracking system according to claim 3, wherein the temporal sequence of values is measured from an initial synchronized starting point of each identification medium, where the initial synchronized starting point is after completion of the data transfer logging the badge on.

In reference to claim 9:

De La Huerga(Column 13, lines 46-50) & (Column 14, lines 15-30) discloses the tracking system according to claim 1, wherein the temporal sequence of values is incremented in equal time increments, where each recommitment period is set forth by a predetermined second period of time.

In reference to claim 19:

De La Huerga (Column 9, lines 19-39) discloses a tracking system wherein the transmitter module is incorporated in any one or more of: an identification badge, a card, or a label, where the identification badge is the security badge and the transmitter module is located within the badge.

In reference to claim 20:

De La Huerga (Column 9, lines 20-29) discloses the tracking system according to claim 19, wherein the identification medium includes any one or more of: a credit card, a dining card, a telephone calling card, a health card; a driver's license; a video store card; a car access card; a computer access card; or a building access card; an identification tag, a key fob, where the tracking system is a security badge identification tag.

In reference to claim 21:

De La Huerga discloses a tracking method for use with a plurality of identification media to selectively provide time-limit access to a resource, comprising:

- Encrypting the temporal sequence of values (Tbn) of the identification media with private keys Kn that are unique to each identification medium, to generate a transmission comprised of encrypted code elements (Tbn)Kn, where the transmission generates a sequence to timestamps at each poll (Column 13, lines 46-50) & (Column 19, lines 17-33) which is encrypted by security badge. (Column 11, lines 55-60)

- Securely storing the private keys of the plurality of identification media, where the private keys are stored in the security verification system (Column 12, lines 33-39)
- Authenticating the transmitted encrypted code elements(Tbn)Kn by creating an authentication table composed of precalculated encrypted code elements for the identification media for the temporal sequence of values (Tbn), and further attempting to match encrypted code elements (TBn)Kn to the precalculated encrypted code elements in the authentication table.

Claim 22 is rejected for the same reasons as claim 11.

In reference to claim 23:

A wireless identification system for use with an identification medium to provide access to a resource, comprising:

- A sequence generator to generate a temporal sequence of values(TBn); where the time generator generates the sequence of values as timestamps (Column 21, lines 45-50) & (Column 19, lines 17-33), and where the code list of encrypted elements is the list of the timestamps and other information on the smartcard used to form the audit trail (Column 19, lines 49-64)
- A private key Kn unique to the identification medium (Column 11, lines 10-16)
- An encryptor to receive a temporal sequence value and the private key, and to output an encrypted result; (Column 11, lines 45-51)

- A transmitter module secured to the identification medium to receive the encrypted result and to output a wireless signal. (Column 11, lines 30-37) & (Column 11, lines 55-59)
- A receiver module to receive the wireless signal and output the encrypted result (Column 11, lines 30-37) & (Column 11, lines 55-59)
- An authenticator, to receive the encrypted result and the private key Kn, and to output an access authorization signal. (Column 12, lines 3-6)

In reference to claim 24:

De La Huerga (Column 4, lines 44-52) discloses the wireless identification system according to claim 23, for use with a plurality of identification media, each identification medium including a transmitter module and a unique private key for transmitting one or more of the encrypted results to the receiver module for authentication, where tracking system is used with a plurality of security badges, each equipped with a unique private key (Column 11, lines 10-15).

In reference to claim 25:

De La Huerga(Column 12, lines 33-39) discloses the wireless identification system according to claim 24, wherein the authenticator stores private keys of the plurality of identification media, where the authenticator is the security verification system, which stores the private keys needed to authenticate a holder of the security badge.

Claim 26 is rejected for the same reasons as claim 10.

In reference to claim 27:

De La Huerga(Column 4, lines 15-39) discloses the wireless identification system according to claim 26 wherein the future encrypted results are distributed to a remote authenticator to enable time-limited access to a resource.

Claim 28 is rejected for the same reasons as claim 8.

Claim 29 is rejected for the same reasons as claim 9.

In reference to claim 30:

De La Huerga(Column 13, lines 46-50) discloses the wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal periodically.

In reference to claim 31:

De La Huerga(Column 10, lines 21-30) discloses the wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal upon external stimulus, wherein the external stimulus is any one or more of: a mechanical switch, a motion detector, a light detector, or a sound detector, where the external stimulus is an activation button or latch.

Claim 33 is rejected for the same rationale as the rejection of claim 16.

Claim 34 is rejected for the same rationale as the rejection of claim 17.

Claim 35 is rejected for the same rationale as the rejection of claim 18.

Claim 36 is rejected for the same reasons as claim 19.

Claim 37 is rejected for the same reasons as claim 20.

Claim 38 is rejected for the same reasons as claim 5.

Claim 39 is rejected for the same reasons as claim 11.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 10-18, 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over De la Huerga.

In reference to claim 10:

De La Huerga(Column 14, lines 59-67) discloses the tracking system according to claim 7, wherein the authenticator creates an authentication table composed of precalculated code elements for every identification medium, and further attempts to match the encrypted code elements transmitted by the transmitter module to the precalculated code elements in the authentication table, where the encrypted code elements received are encrypted and then decrypted to be compared.

De La Huerga however, fails to specifically disclose a system wherein the code elements are encrypted and precalculated.

The examiner takes official notice that comparing encrypted code elements for a match in a verification process was well known at the time of invention. Examples of this are comparing digital signatures, Message Authentication Codes, or Hashes.

It would have been obvious to one of ordinary skill in the art at the time of invention to compare precalculated encrypted code elements, in order to avoid the extra computation of decryption when data from the smart card is received, and further to allow the extra pre-calculation of the encrypted code element to be performed at a more convenient time for the server such as a period where traffic were less.

In reference to claim 11:

De La Huerga discloses the tracking system according to claim 10, wherein the server encrypts the temporal sequence of values(TBn), the timestamps (Column 19, lines 17-33) denoted in an audit trail (Column 19, lines 53-63)

and an offset value (Ton) for each identification medium, where the offset value is the interval in the periodic polling (Column 14, lines 20-29), with a corresponding unique private key Kn to generate a list of authentication codes, EN, as represented by the following expression:

En = (Tbn + Ton)Kn

(Column 13, lines 53-60), where the periodic transmissions that are timestamped in the security badge are also encrypted with the private key.

In reference to claim 12:

De La Huerga(Column 19, lines 53-63) discloses the tracking system according to claim 11, wherein the temporal resolution of the authentication table exceeds the transmission cycle of the transmitter module, where if the temporal resolution, the time at which a refresher transmission, exceeds the transmission cycle of the module, the transmission may be dropped or be connected through a new transmission.

In reference to claim 13:

De le Huerga discloses all of claim 13 except a system wherein the temporal resolution of the authentication table is approximately one second and wherein the transmission cycle is ten seconds.

De le Huerga(Column 19, lines 53-63) instead discloses a "preset period of time" which if the association has not been refreshed, then the connection is terminated.

It would have been obvious to one of ordinary skill in the art at the time of invention to have the preset period of polling and the transmission cycle to be within any reasonable time frame in order to continually assess and establish the status of the connection.

In reference to claim 14:

De La Huerga(Column 16, 5-16) discloses the tracking system according to claim 11, wherein the transmitter module transmits at least one encrypted code element to the receiver module as a packet and wherein the packet includes: a preamble field and a payload field, where the preamble field contains the KEY ID tag and also allows authenticator to determine what kind of signal the transmission is.

De La Huerga however, fails to explicitly disclose the use of a checksum field in the transmission.

The examiner takes official notice that sending a checksum with a transmission or communication was known at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a checksum in the transmission with the encrypted code, in order to determine in a quick manner, if the transmission is complete, or had been altered.

In reference to claim 15:

De La Huerga (Column 16, lines 15-32) discloses the tracking system according to claim 14, wherein the preamble field contains data bits indicating that the packet is originating from a valid identification medium

The payload field contains an encrypted code element (Tbn)Kn, where (Tbn)Kn is recorded as the timestamp as part of the record, which is later encrypted by a public or private key. (Column 16, lines 15-32) & (Column 19, lines 15-36)

De La Huerga fails to explicitly disclose a tracking system wherein the checksum field allows for checking transmission integrity. Claim 15 is rejected for the same combination rendered in claim 14.

In reference to claim 16:

De La Huerga(Column 19, lines 49-63) discloses the tracking system according to claim 11 , wherein the temporal sequence of values (TBn) is represented by the following expression;

(TBn) = Tsystem – Tncreation

- where Tsystem represents current time for the server, and TnCreation represents a creation time of the identification medium referenced to a same time standard as Tsystem; where Tsystem is the moment at which the security badge is re-polled, and re-recorded with a new timestamp. (Column 19,lines 15-36)
- and wherein the server stores Tncreation for each identification medium, where TnCreation is the period at which the logon was initially made. Recommitment signals are recorded as relative to the logon where logon is zero. (Column 13, lines 35 – Column 14, line 12)

In reference to claim 17:

De La Huerga(Column 14, lines 20-30) discloses the tracking system according to claim 16, wherein the server establishes a clock synchronization window for the list of authentication codes, EN, to account for time drift between the current time of the identification medium and a current time of the server, where the time drift is the second period of time during which the security badge has the chance to refresh the signal. This synchronization window or window of opportunity is what allows two devices to remain in synch.

In reference to claim 18:

De La Huerga (Column 13, lines 35 – Column 14, line 12)

discloses the tracking system according to claim 17, wherein the clock synchronization window is centered around the current time (TBn) of the identification medium, as shown by the following expressions, where Ton is the second period of time, or the open window with which the connection may be refreshed, and Epsilon is the period at which the signal is received:

En1 = (TBn + Ton),

En2 = (TBn + Ton – Epsilon)Kn, and

En3 = (TBn + Ton + Epsilon)Kn

- Wherein En1 is the authentication code when the identification medium is in general synchrony with the server, where the signal is received at the second period of time.
- Wherein En2 is the authentication code when the identification medium lags the server, where the signal is received after the second period of time, lagging the server.
- Wherein En3 is the authentication code when the identification medium leads the server, where in case three, the signal is received before the second period of time is complete, leading the server.
- Wherein Epsilon is the resolution of the temporal sequence of values (TBn), where the resolution of values occurs when the signal from the security badge is successfully refreshed.

Claim 32 is rejected for the same reasons as claim 10.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

April 26th 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100